Trusted Systems

James Green, Chief Operating Officer

Trusted Systems

“If the organization gets into a lawsuit, it has to produce certain records to support its case”

Forget finding it

Forget how long you should have kept it

How can you show that records you put into an electronic system are the records you will get out?

Evidentiary Foundations

Authentic Digital Records:
Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

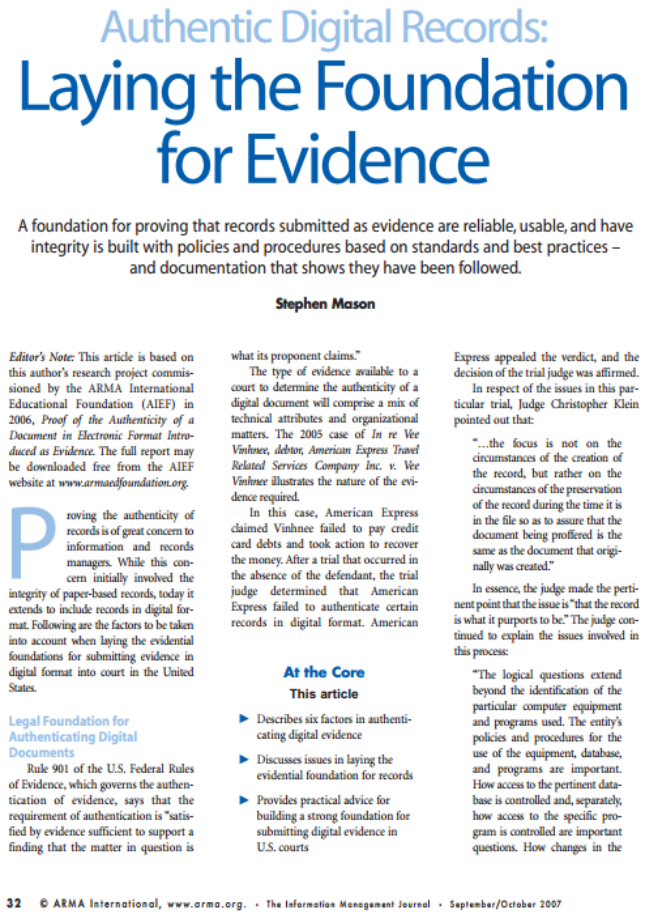
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

Evidentiary Foundations Case Study

The Story



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

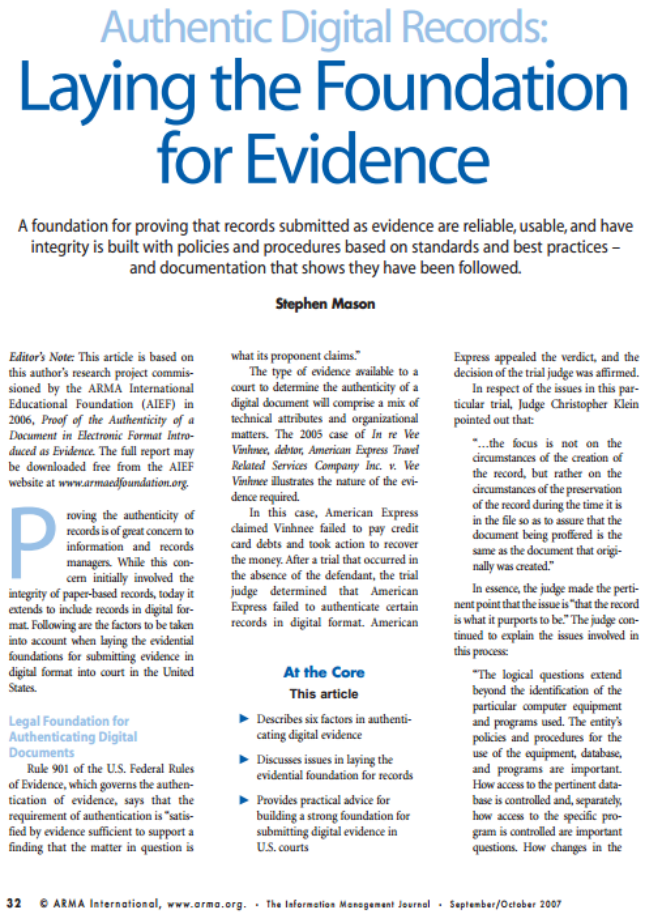
> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

American Express

Evidentiary Foundations Case Study
The Lesson



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

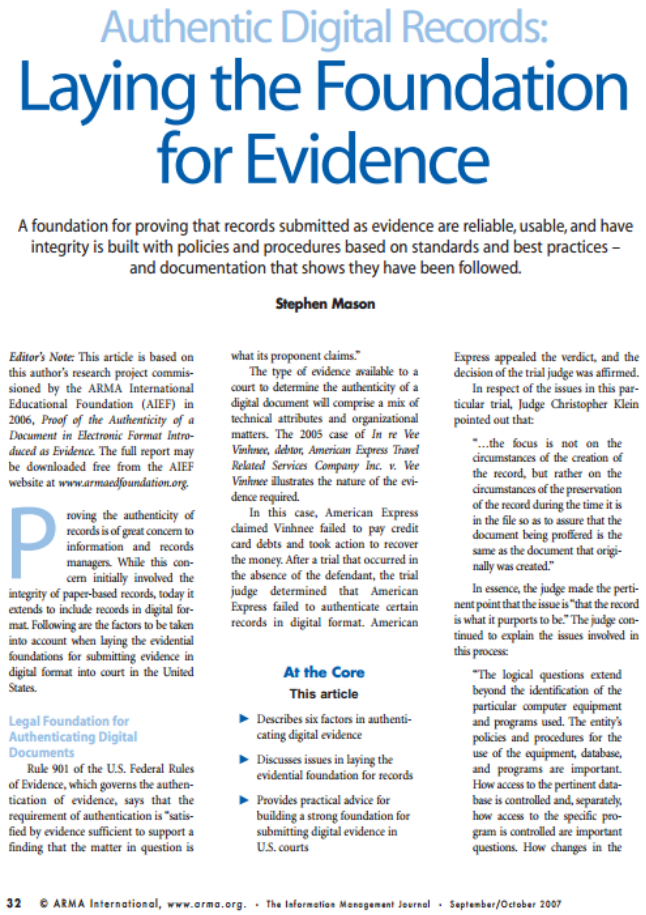
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- Witness not credible
- Policies and procedures not provided

Trusted Electronic Records



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

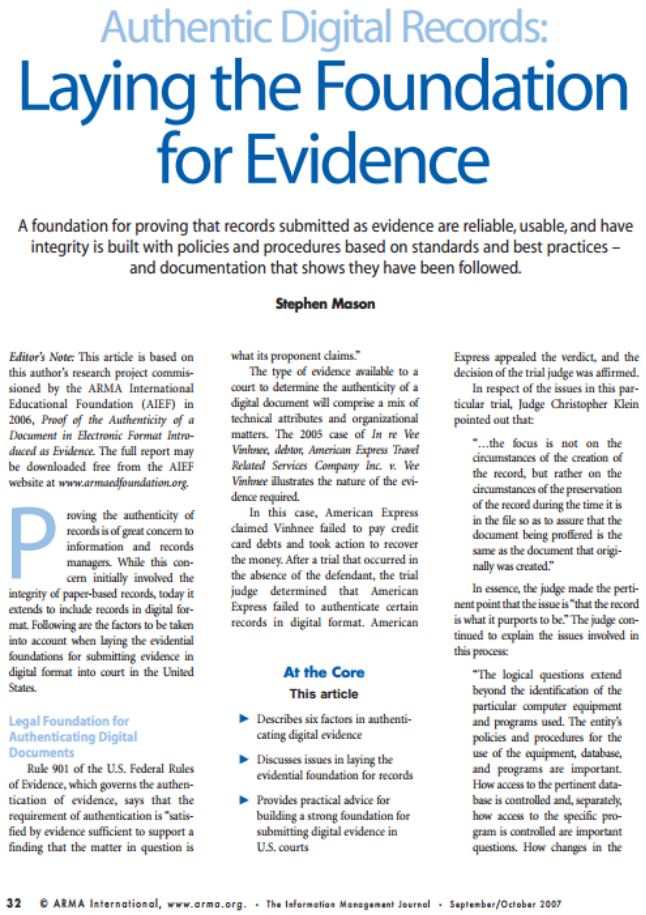
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- Outlines 11 Evidentiary Foundations for Electronic Records
- These were established by Edward Imwinkeleried
- They have been used multiple times in U.S. cases and abroad

Evidentiary Foundation 1-3



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

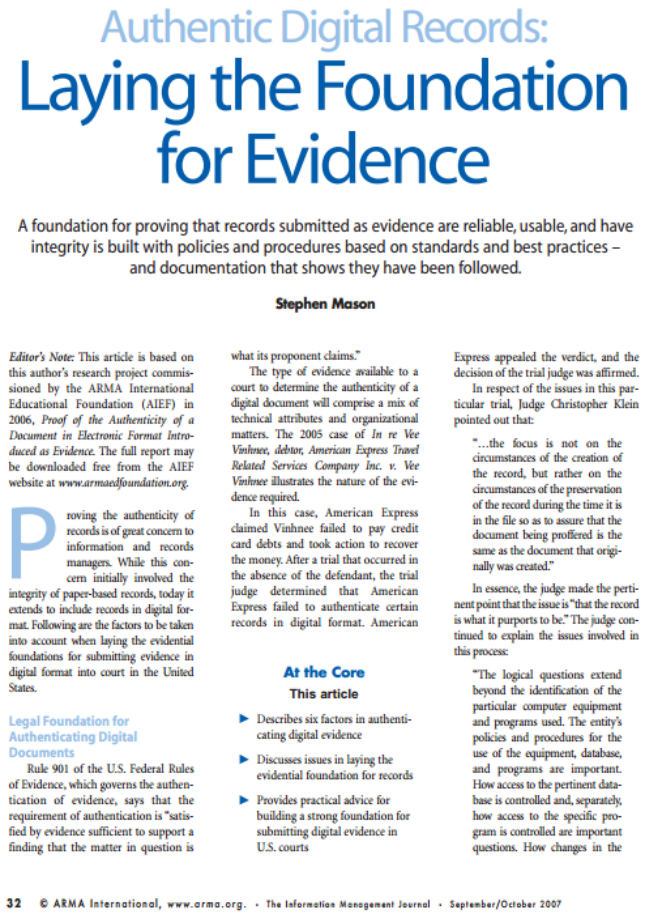
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- The business uses a computer.
- The computer is reliable.
- The business has developed a procedure for inserting data into the computer.

Evidentiary Foundation 4



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

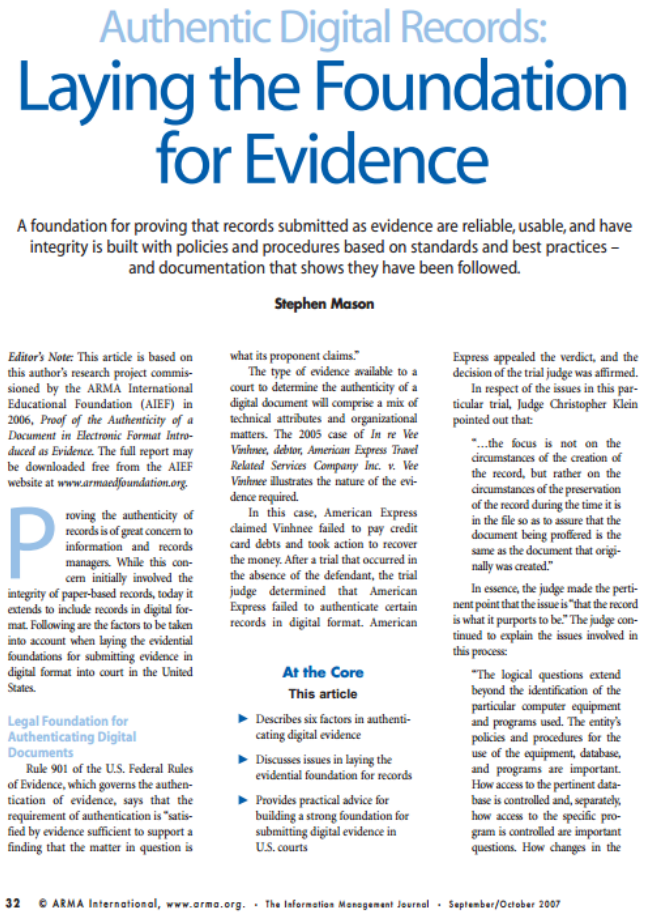
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- The **procedure** has built-in safe-guards to ensure accuracy and identify errors.
  - Procedures
    - Access control
    - Logging of changes
    - Backup practices
    - Audit procedures

Evidentiary Foundation 5-6



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

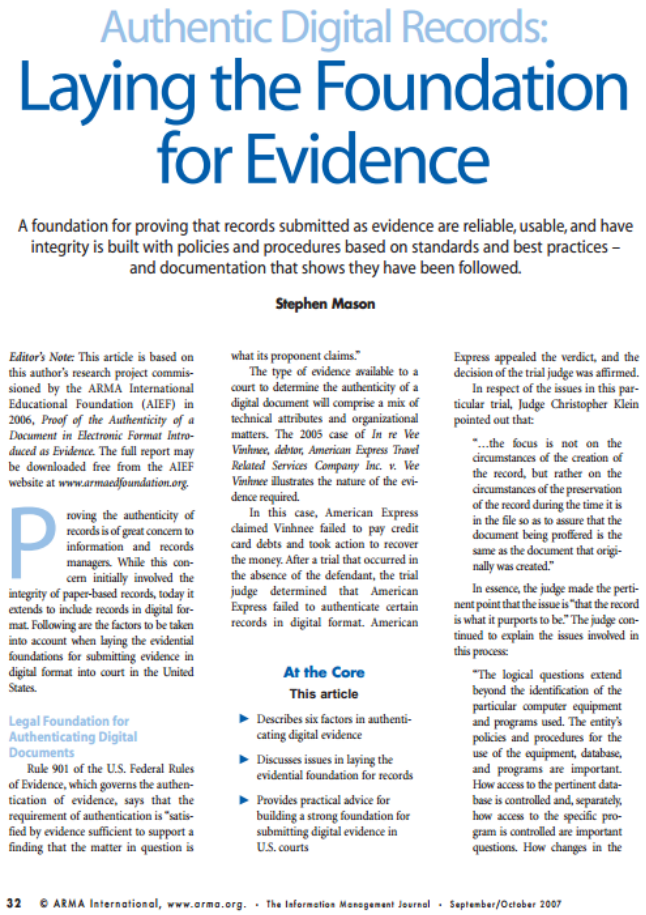
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- The business keeps the computer in a good state of repair.
- The witness had the computer readout certain data.

Evidentiary Foundation 7



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

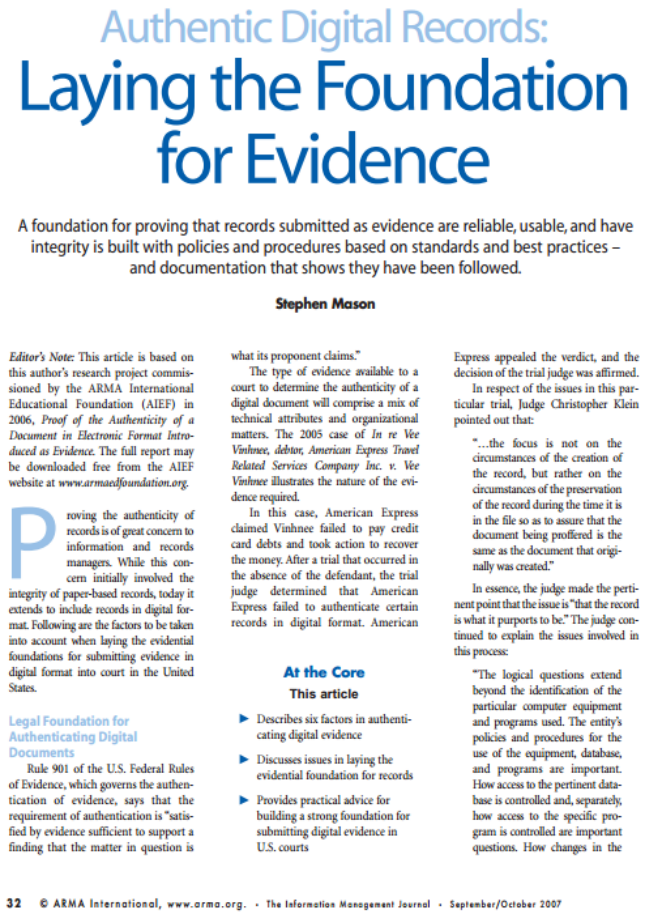
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- The witness used the proper procedures to obtain the readout.
  - Search Method
  - Version Control

Evidentiary Foundation 8-10



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

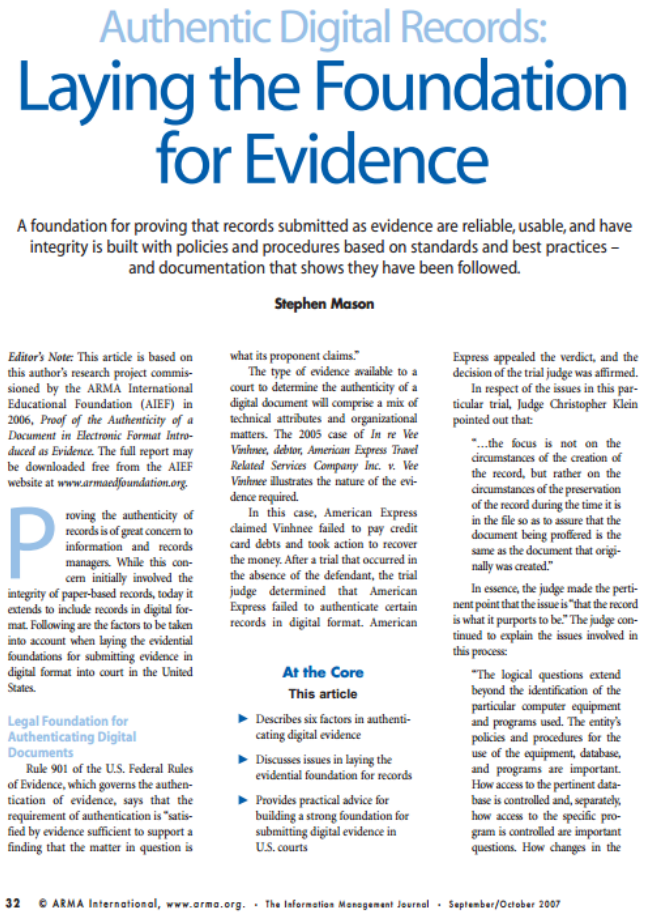
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- The computer was in working order at the time the witness obtained the readout.
- The witness recognizes the exhibit as the readout.
- The witness explains how her or she recognizes the readout.

Evidentiary Foundation 11



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

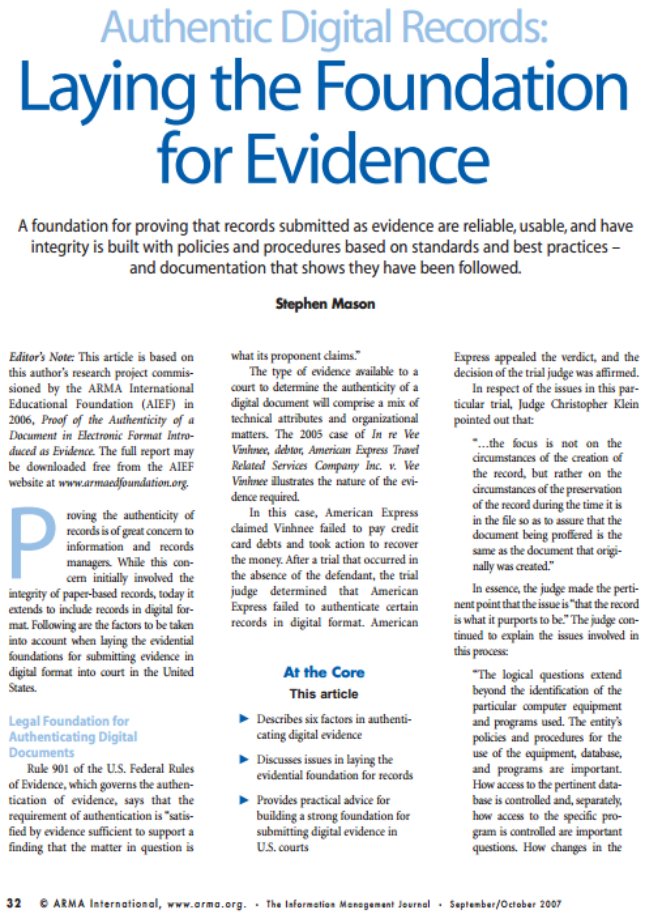
At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

Evidentiary Foundations Summary



Authentic Digital Records:

Laying the Foundation for Evidence

A foundation for proving that records submitted as evidence are reliable, usable, and have integrity is built with policies and procedures based on standards and best practices – and documentation that shows they have been followed.

Stephen Mason

Editor's Note: This article is based on this author's research project commissioned by the ARMA International Educational Foundation (AIEF) in 2006, *Proof of the Authenticity of a Document in Electronic Format Introduced as Evidence.* The full report may be downloaded free from the AIEF website at *www.armaedfoundation.org.*

Proving the authenticity of records is of great concern to information and records managers. While this concern initially involved the integrity of paper-based records, today it extends to include records in digital format. Following are the factors to be taken into account when laying the evidential foundations for submitting evidence in digital format into court in the United States.

Legal Foundation for Authenticating Digital Documents

Rule 901 of the U.S. Federal Rules of Evidence, which governs the authentication of evidence, says that the requirement of authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

The type of evidence available to a court to determine the authenticity of a digital document will comprise a mix of technical attributes and organizational matters. The 2005 case of *In re Vee Vinhnee, debtor, American Express Travel Related Services Company Inc. v. Vee Vinhnee* illustrates the nature of the evidence required.

In this case, American Express claimed Vinhnee failed to pay credit card debts and took action to recover the money. After a trial that occurred in the absence of the defendant, the trial judge determined that American Express failed to authenticate certain records in digital format. American Express appealed the verdict, and the decision of the trial judge was affirmed.

In respect of the issues in this particular trial, Judge Christopher Klein pointed out that:

> "…the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created."

In essence, the judge made the pertinent point that the issue is "that the record is what it purports to be." The judge continued to explain the issues involved in this process:

> "The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the

At the Core

This article

- Describes six factors in authenticating digital evidence
- Discusses issues in laying the evidential foundation for records
- Provides practical advice for building a strong foundation for submitting digital evidence in U.S. courts

- Implement a reliable system
- Develop comprehensive procedures
- Follow the procedures
- Choose a credible witness

Trusted System (GC §12168.7)

- “a combination of techniques, policies, and procedures for which there is no plausible scenario in which a document retrieved from or reproduced by the system could differ substantially from the document that is originally stored.”
- State of California – Secretary of State
  - Developed regulations CCR §22620.1-8
- “Trustworthy Electronic Document or Record Preservation”

CCR §22620.1 - Purpose

- Identify uniform statewide standards for recording, storing, and reproducing records in electronic media.
- Applies to agencies required by statute to follow GC §12168.7

CCR §22620.2 – Applicability of Electronic Document Record Standards

- All electronic records that are the official record
  - Designate electronic or hard-copy in your retention policy
- Does not apply to hard-copy records

CCR §22620.3 Definitions

- AIIM
- ANSI
- ISO
- PDF/A
- Trusted Systems
- Official Documents

CCR §22620.4 Official Document or Record Storage Using Electronic Technologies

- Must use a trusted system for “official” electronic records
- Must implement for all new information since August 2012

CCR §22620.5 – Business Practice Documentation

- Document procedures associated with creation, management, and storage
  - How are record supposed to be created or captured?
  - How is the retention schedule supposed to be managed? How do you audit the system?
  - How is the system backed up? How do you ensure the information is unalterable?
- In addition to a retention schedule, develop and adopt a formal record retention policy

CCR §22620.6 – Electronic File Compression

- Use ITU Group 4, LZW, JPEG, JPEG 2000, JBIT, or other output format with no proprietary alterations

CCR §22620.7 – Trusted Storage of Official Electronic Documents or Records

- Keep at least two copies of every record
- Keep the copies at geographically separate locations
- Ensure that at least one copy of the file is unalterable
- WORM (Write Once Read Many)
  - Optical
  - Tape
  - Hard-Drive (w/ Encryption)

CCR §22620.8 – Electronic File Format for Preservation of Converted Official Documents or Records

- Use PDF/A or TIFF (Standard) for documents
- Use JPG, PNG, or GIF for photos
- Avoid PDF or TIFF (Non-Standard)
- Avoid DOC, XLS, PPT, MSG

Summary of CCR §22620

1. Create and use a records policy
2. Create at least two copies of the record
3. Use unalterable storage (for the life the record)
4. Regularly perform an independent audit of the system
5. Use non-proprietary record formats

Trusted Systems and the Cloud

- Hosted versus SaaS Environment
- Security
- Immutability
  - Storage Media, Encryption, Hash Values
- Auditability

Vendors and Trusted Systems

- Most vendors are familiar with Trusted Systems
- Expect to purchase additional hardware and professional services

Cost and Compliance

- No state audit or penalties for non-compliance
- The cost of non-compliance is your liability from a judge questioning the validity of your records
- Liability costs for smaller organizations may be less than compliance costs
- Remember, judges are human too

Next Steps

- Develop a records policy that accounts for the regulations in the GC
- Update your records policy to reflect the location of “official records”
- Make sure you have offsite backups of electronic records
- Make sure that your information is unalterable during its lifecycle
- Audit the system on a regular basis to ensure compliance with records policy

Questions?

James Green, Chief Operating Officer

ECS Imaging, Inc.
Your World Class Laserfiche Provider

(915) 787-8768

james@ecsimaging.com

www.ecsimaging.com